What is claimed is:

1. A method comprising:

auditing less than all of a number of transactions within a computing device, wherein auditing of one of the number of transactions comprises:

storing at least one attributes of the one of the number of transactions into an audit log within a memory of the computing device;

encrypting the audit log based on an encryption key that is generated and stored within the computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

2. The method of claim 1, wherein auditing of one of the number of transactions further comprises generating a signature of a value of an audit counter with the signature key.

3. The method of claim 2, wherein auditing of one of the number of transactions further comprises appending the integrity metric, the signature of the integrity metric, the signature of the value of the audit counter and the value of the audit counter to the audit log.

4. A method comprising:

selectively auditing a number of transactions between a computing device and a separate device based on a type for the number of transactions, wherein selectively auditing of the number of transactions includes securely storing at least one attribute of selected audited transactions within the computing device.

5. The method of claim 4, wherein securely storing the at least one attribute of one of the selected audited transactions comprises:

storing at least one attribute of the selected audited transaction into an audit log into a memory in the computing device; and

encrypting the audit log based on an encryption key that is generated and stored within the computing device.

6. The method of claim 4, wherein securely storing the at least one attribute comprises:

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

7. The method of claim 6, wherein securely storing the at least one attribute comprises:

incrementing an audit counter; and

storing a value of the audit counter, the integrity metric and the signature in the audit log.

8. The method of claim 4, wherein the at least one attribute is selected from a group consisting of the type of transaction, a monetary amount of the transaction and a time of the transaction.

9. A method comprising:

receiving events based on communications between a computing device and a separate entity;

auditing less than all of the events based on a type for the events, wherein the auditing comprises:

opening an audit session upon receipt of one of the events to be audited;

incrementing a value of an audit counter after the audit session is open;

storing attributes of the events to be audited in an audit log; and

performing the following operations after the audit session is closed:

generating a hash of the audit log;

generating a digital signature of the hash and the value of the audit counter based on a first encryption key;

storing the hash, the value of the audit counter and the digital signature in the audit log; and

encrypting the attributes of the events store in the audit log with a second encryption key that is different from the first encryption key.

10. The method of claim 9, wherein receiving the events based on the communications between the computing device and the separate entity comprises receiving the events based on transactions between the computing device and the separate entity.

11. The method of claim 9, wherein the attributes are selected from a group consisting of the type of transaction, a monetary amount of the transaction and a time of the transaction.

12. An apparatus comprising:

a control logic to selectively audit transactions between the apparatus and a separate entity based on a type for the transactions; and

an encryption logic to encrypt an audit log that includes at least one attribute of one of the selectively audited transactions.

13. The apparatus of claim 12 further comprising a memory to securely store the at least one attribute in an audit log.

14. The apparatus of claim 13 further comprising a hashing logic to generate an integrity metric of the audit log.

15. The apparatus of claim 14 further comprising:

a key generation logic to generate a signature key; and

a signature logic to generate a signature of the integrity metric based on the signature key to store the signature of the integrity metric in the audit log.

16. The apparatus of claim 15, wherein the selectively audited transactions include a number of audit events, the control logic is to activate an audit session after receipt of an audit event in the apparatus when no audit session is active in the apparatus.

17. The apparatus of claim 16 further comprising an audit counter, wherein the control logic is to increment a value of the audit counter after activation of the audit session.

18. The apparatus of claim 16, wherein the signature logic is to generate a signature of the audit counter based on the signature key to store the signature of the audit counter in the audit log.

19. A system comprising:

an input/output (I/O) logic to receive and transmit data of transactions into the system;

a flash memory;

a processor to generate events based on execution of an application to process the data; and

a cryptographic processing module to selectively audit the events, the cryptographic processing module to securely store an audit log of the selectively audited events.

20. The system of claim 19, wherein the cryptographic processing module is to securely store the audit log based on an encryption of the audit log.

21. The system of claim 20, wherein the cryptographic processing module is to generate an integrity metric of the audit log and to generate a signature of the integrity metric with a signature key that is generated and stored within the cryptographic processing module.

22. The system of claim 21, wherein the cryptographic processing module is to open an audit session after receipt of one of the selectively audited events when no audit session is active in the system.

23. The system of claim 21, wherein the cryptographic processing module comprises an audit counter, wherein the cryptographic processing module is to increment the audit counter after the audit session is open.

24. The system of claim 21, wherein the cryptographic processing module is to store a value of the audit counter, the signature and the integrity metric in the audit log.

25. The system of claim 19, wherein the cryptographic processing module is to securely store the audit log of the selectively audited events in the flash memory.

26. The system of claim 19, wherein the cryptographic processing module is to securely store the audit log of the selectively audited events in a memory internal to the cryptographic processing module.

27. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

auditing less than all of a number of transactions within a computing device, wherein auditing of one of the number of transactions comprises:

storing at least one attributes of the one of the number of transactions into an audit log within a memory of the computing device;

encrypting the audit log based on an encryption key that is generated and stored within the computing device;

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

28. The machine-readable medium of claim 27, wherein auditing of one of the number of transactions further comprises generating a signature of a value of an audit counter with the signature key.

29. The machine-readable medium of claim 28, wherein auditing of one of the number of transactions further comprises appending the integrity metric, the signature of the integrity metric, the signature of the value of the audit counter and the value of the audit counter to the audit log.

30. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

selectively auditing a number of transactions between a computing device and a separate device based on a type for the number of transactions, wherein selectively auditing of the number of transactions includes securely storing at least one attribute of selected audited transactions within the computing device.

31. The machine-readable medium of claim 30, wherein securely storing the at least one attribute of one of the selected audited transactions comprises:

storing at least one attribute of the selected audited transaction into an audit log into a memory in the computing device; and encrypting the audit log based on an encryption key that is generated and stored within the computing device.

32. The machine-readable medium of claim 30, wherein securely storing the at least one attribute comprises:

generating an integrity metric of the audit log; and

generating a signature of the integrity metric with a signature key that is generated and stored within the computing device.

33. The machine-readable medium of claim 32, wherein securely storing the at least one attribute comprises:

incrementing an audit counter; and

storing a value of the audit counter, the integrity metric and the signature in the audit log.

34. A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

receiving events based on communications between a computing device and a separate entity;

auditing less than all of the events based on a type for the events, wherein the auditing comprises:

opening an audit session upon receipt of one of the events to be audited;

incrementing a value of an audit counter after the audit session is open;

storing attributes of the events to be audited in an audit log; and

performing the following operations after the audit session is closed:

generating a hash of the audit log;

generating a digital signature of the hash and the value of the audit counter based on a first encryption key;

storing the hash, the value of the audit counter and the digital signature in the audit log; and

ncrypting the attributes of the events store in the audit log with a second encryption key that is different from the first encryption key.

35. The machine-readable medium of claim 34, wherein receiving the events based on the communications between the computing device and the separate entity comprises receiving the events based on transactions between the computing device and the separate entity.

36. The machine-readable medium of claim 35, wherein the attributes are selected from a group consisting of the type of transaction, a monetary amount of the transaction and a time of the transaction.